Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-13. (Cancelled)

14. (Currently Amended) A method of performing a cryptographic protocol between a first electronic entity and a second electronic entity in order to resist ~~to~~ an attack against the second electronic entity, comprising the steps of:

applying a message to both first and second electronic entities,

applying a first chain of operations to the message within the first electronic entity, so as to obtain a result,

determining a second chain of operations ~~derived~~ from the first chain of operations, ~~and applying the second chain of operations to the message within the second electronic entity so as to obtain a resultant message,~~ the step of determining the second chain of operations from the first chain of operations comprising randomly selecting, for at least a part of the ~~operations of the~~ first chain of operations, to perform, as the second chain of operations, either the at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or the at least a part of the first chain of

operations in a complemented state, the second chain of operations comprising some operations of the first chain of operations which are performed in the same state and some other operations of the first chain of operations which are performed in a complemented state;

applying the second chain of operations to the message within the second electronic entity so as to obtain a resultant message, the step of applying comprising ~~outputting~~ selecting to output as the resultant message, depending on ~~responsive to~~ the step of randomly selecting, one of either a last operation of the second chain of operations in a same state or the last operation of the second chain of operations in a complemented state ~~a last operation of the first chain of operations, or a complemented result of the second chain of operations~~, and

comparing the resultant message obtained from the second chain of operations to the result of the first chain of operations.

15. (Currently Amended) The method of claim 14, wherein the at least a part of the first chain of operations ~~which can be performed in a complemented state~~ comprises an exclusive OR.

16. (Currently Amended) The method of claim 14, wherein the at least a part of the first chain of operations ~~which can be performed in a complemented state~~ comprises an operation of permutation of the bits of said message or of an intermediate result obtained on carrying out said second chain of operations until the operation of permutation of the bits of said message.

17. (Currently Amended) The method of claim 14, wherein the at least a part of the first chain of operations ~~which can be performed in a complemented state~~ comprises an operation of indexed access to a table.

18. (Currently Amended) The method of claim 14, wherein the at least a part of the first chain of operations ~~which can be performed in a complemented state~~ comprises an operation which is stable with respect to the application of an exclusive OR function.

19. (Currently Amended) The method of claim 18, wherein the at least a part of the first chain of operations ~~which can be performed in a complemented state~~ is an operation of transfer of the message or of an intermediate result obtained by carrying out said second chain of operations until the operation of transfer of the message, from one location to another one in a storage space.

20. (Currently Amended) The method of claim 14, wherein the step of randomly selecting ~~to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state~~ comprises identifying a series of several parts within the first chain of operations and comprises randomly selecting, for each of said ~~a~~ series of several parts of the first chain of operations, to perform either such part in a normal state or in a complemented state.

21. (Currently Amended) The method of claim 20, wherein the step of randomly selecting ~~to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state~~ comprises identifying a series of operations within each of said series of several parts of the first chain of operations, comprises randomly selecting, for each of said ~~a~~ series of operations of said series of several parts of the first chain of operations, ~~adjacent or not,~~ to perform ~~either~~ such operation either in a normal state or in complemented state.

22. (Currently Amended) The method of claim 20, wherein the step of randomly selecting ~~to perform either the at least a part of the first chain of operations or the at~~

~~least a part of the first chain of operations in complemented state~~ is conducted depending on the state of a random parameter generated for each such~~the at least a~~ part of the first chain of operations and comprises updating a complementation counter, and the step of selecting to output ~~outputting~~ as the resultant message is decided depending on the state of the complementation counter.

23. (Currently Amended) The method of claim 20, wherein the step of randomly selecting ~~to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a complemented state~~ is conducted depending on the state of a random parameter generated for each such ~~the at least a~~ part of the first chain of operations and comprises transmitting, for each operation of the at least part of the first chain of operations, information for deciding the step of outputting the resultant message.

24. (Currently Amended) The method of claim 20, wherein the step of randomly selecting ~~determining and applying the similar chain of operations~~ comprises the computing of a parameter which is equal to a difference between the number of times when an operation of the first chain of operations was performed in the same state as in the

first chain of operations and the number of times when other ones ~~another one~~ of the first chain of operations of the chain was performed in complemented state, and when this difference exceeds a given threshold, the decision to perform a next operation ~~one of the second chain of operations~~ in a complemented state or not is taken so as to decrease this difference.

25. (Currently Amended) The method of claim 14, wherein the step of randomly selecting ~~determining the second chain of operations~~ comprises selecting randomly to perform either the whole of the first chain of operations in the same state as in this first chain of operations or the whole of the first chain of operations ~~or all of the chain~~ in complemented state selectively followed by a final complementing step.

26. (Currently Amended) The method of claim 25, wherein the step of randomly selecting ~~and applying the second chain of operations~~ comprises computing a parameter which is the difference between the number of times when the operations of the first chain of operations were performed in normal state and the number of times when such operations of the first chain of operations were performed in a complemented state, and when this difference exceeds a given threshold, ~~the~~ a decision to perform a next one of the second chain of

operations in a complemented state is taken so as to decrease this difference.

27. (Previously Presented) The method of claim 14, wherein the complemented state of the at least a part of the first chain of operations is obtained by a complementation carried out byte by byte.

28. (Previously Presented) The method of claim 14, wherein the complemented state of the at least a part of the first chain of operations is obtained by a complementation carried out bit by bit.

29. (Previously Presented) The method of claim 14, wherein the step of determining the second chain of operations further comprises a step of determining a permutation of the order of successive commutative operations in the first chain of operations.

30. (Previously Presented) The method of claim 29, wherein the step of determining a permutation of the order of successive commutative operations is carried out randomly.

31. (Currently Amended) The method of claim 21, wherein the step of randomly selecting ~~to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in a~~

~~complemented state~~ is conducted depending on the state of a random parameter generated for each operation of the at least a part of the first chain of operations and comprises updating a complementation counter, and selecting the output ~~outputting~~ as the resultant message is decided depending on the state of the complementation counter.

32. (Currently Amended) The method of claim 20, wherein the step of randomly selecting ~~to perform either the at least a part of the first chain of operations or the at least a part of the first chain of operations in complemented state~~ is conducted depending on the state of a random parameter generated for each of the several parts ~~the at least a part~~ of the first chain of operations and comprises transmitting, for each operation of the at least part of the chain of operations, information for deciding the step of outputting the resultant message.

33. (Currently Amended) The method of ~~claim 20~~ claim 21, wherein the step of randomly selecting ~~determining and applying the similar chain of operations~~ comprises the computing of a parameter which is equal to a difference between the number of times when an operation of the first chain of operations was performed and the number of times when another one of the first chain of operations of the chain was

performed in complemented state, and when this difference exceeds a given threshold, ~~the~~ a decision to perform a next operation of the second chain of operations in a complemented state is taken so as to decrease this difference.